UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,543	03/01/2002	Peter M. Rigstad	3COM-3828.MCD.US.P	5432

7590 04/04/2006

WAGNER, MURABITO & HAO LLP
Two North Market Street
Third Floor
San Jose, CA 95113

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/090,543	RIGSTAD ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23,24,26-35 and 40-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *23,24,26-35 and 40-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 14 September 2005.

2. Claims 23, 24, 26-35 and 40-63 are pending in the application.

3. Claims 23, 24, 26-35 and 40-63 have been rejected.

4. Claims1-22, 25 and 36-39 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 14 September 2005 has been entered.

Response to Arguments

6. Applicant's arguments with respect to claims 23, 24, 26-35 and 40-63 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

7. Claim 26 is objected to because of the following informalities: grammatical error. There is a semicolon at the end of claim 26 instead of a period. The semicolon should be replaced with a period. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 23, 26-30, 32, 33, 40, 41, 43-46, 48 and 49 are rejected under 35 U.S.C. 102(e) as being anticipated by Wong et al et al U.S. Patent No. 6,389,419 B1.

As to claims 23, 33, 41 and 49, Wong et al discloses that the host device routes the data to the firewall device is to be processed by the hardware-implemented firewall [column 1 line 58 to column 2 line 17]. Wong et al discloses that the routing takes place at a physical layer in the data stack [column 1 line 58 to column 2 line 17].

As to claim 26, Wong et al discloses a method of providing security in a network having a network interface device that makes a network connection without a firewall capability in the communication interface device that is required by the network for data transfer between the network and a host device using the network interface device, the method comprising:

a) allowing a connection to the network to be established when the host device uses the network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to the host device [column 2 line 18 to column 3 line 44];

b) receiving data from the network over the connection establish via the communication interface device [column 2 line 18 to column 3 line 44];

c) processing the data with the hardware implemented firewall [column 2 line 18 to column 3 line 44]; and

d) transferring the data to the host device, wherein the data is processed by the hardware implemented firewall [column 2 line 18 to column 3 line 44]; and

e) performing a configuration integrity check of a software component on a host device, wherein the configuration integrity check is performed before the network connection is allowed, wherein the connection is allowed if the configuration integrity check passes [column 2 line 18 to column 3 line 44].

As to claim 27, Wong et al discloses that e) comprises performing the configuration integrity check by performing a hash on the software component to produce a hash value and comparing the hash value with a stored hash value [column 2 line 18 to column 3 line 44].

As to claims 28 and 44, Wong et al discloses that the stored hash value resides on the firewall device [column 2 line 18 to column 3 line 44].

As to claims 29 and 45, Wong et al discloses the method further comprising:

f) sending an alert if the configuration integrity check fails [column 5 line 59 to column 6 line 37].

As to claims 30 and 46, Wong et al discloses the method further comprising:

g) storing an alert if the configuration integrity check fails [column 5 line 59 to column 6 line 37].

As to claims 32 and 48, Wong et al discloses transferring data to be transferred over the network by the communication interface device to the firewall device [column 2 line 18 to column 3 line 44]. Wong et al discloses processing the data with the hardware-implemented

firewall [column 2 line 18 to column 3 line 44]. Wong et al discloses that the data is processed by the hardware-implemented firewall before it is transferred over the network connection established via the communication interface device [column 2 line 18 to column 3 line 44].

As to claim 40, Wong et al discloses a method of providing security in a network having a network interface device that makes a network connection without a firewall capability in the communication interface device that is required by the network for data transfer between the network and a host device using the network interface device, the method comprising:

allowing a connection to the network to be established when the host device uses the network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to the host device [column 2 line 18 to column 3 line 44];

receiving data from the network over the connection establish via the communication interface device [column 2 line 18 to column 3 line 44];

processing the data with the hardware implemented firewall [column 2 line 18 to column 3 line 44];

transferring the data to the host device, wherein the data is processed by the hardware implemented firewall [column 2 line 18 to column 3 line 44]; and

performing a configuration integrity check of a software component on the host device by performing a hash on the software component to produce a hash value and comparing the hash value with a stored hash value [column 2 line 18 to column 3 line 44].

As to claim 43, Wong et al discloses that the configuration integrity check is performed before the network connection is allowed and wherein the connection is allowed only if the configuration integrity check passes [column 2 line 18 to column 3 line 44].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 24, 34, 35, 42, 50-60, 62 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al et al U.S. Patent No. 6,389,419 B1 as applied to claims 26, 40 and 52 above, and further in view of Mayer U.S. Patent No. 7,003,562 B2.

As to claims 24, 42 and 54, Wong et al does not teaching sending policies to the firewall device and that the operation of the hardware implemented firewall is modified.

Mayer teaches sending updated network wide policies to network devices [column 4, lines 5-44].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al so that updated security policies would have been sent to the firewall and the operation of the hardware implemented firewall would have been modified.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al by the teaching of Mayer because it helps pinpoint network deviations [column 2, lines 38-54].

As to claims 34 and 50, Wong et al teaches performing a configuration integrity check of a software component on the host device.

Wong et al does not teaching sending policies to the firewall device and that the operation of the hardware implemented firewall is modified [column 5 line 59 to column 6 line 37].

Mayer teaches sending updated network wide policies to network devices [column 4, lines 5-44].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al so that updated security policies would have been sent to the firewall and the operation of the hardware implemented firewall would have been modified.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al by the teaching of Mayer because it helps pinpoint network deviations [column 2, lines 38-54].

As to claim 35 and 51, Wong et al teaches the method further comprising:

sending an alert if the configuration integrity check fails [column 5 line 59 to column 6 line 37].

As to claim 52, Wong et al discloses a method of providing security in a network having a network interface device that makes a network connection without a firewall capability in the communication interface device that is required by the network for data transfer between the network and a host device using the network interface device, the method comprising:

allowing a connection to the network to be established when the host device uses the network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to the host device [column 2 line 18 to column 3 line 44];

receiving data from the network over the connection establish via the communication interface device [column 2 line 18 to column 3 line 44];

processing the data with the hardware implemented firewall [column 2 line 18 to column 3 line 44];

transferring the data to the host device, wherein the data is processed by the hardware implemented firewall [column 2 line 18 to column 3 line 44];

performing a configuration integrity check of a software component on the host device [column 2 line 18 to column 3 line 44]; and

sending an alert if the configuration integrity check fails [column 2 line 18 to column 3 line 44].

Wong et al does not teaching sending policies to the firewall device and that the operation of the hardware implemented firewall is modified [column 5 line 59 to column 6 line 37].

Mayer teaches sending updated network wide policies to network devices [column 4, lines 5-44].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al so that updated security policies would have been sent to the firewall and the operation of the hardware implemented firewall would have been modified.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al by the teaching of Mayer because it helps pinpoint network deviations [column 2, lines 38-54].

As to claims 53 and 63, Wong et al teaches that the host device routes the data to the firewall device is to be processed by the hardware-implemented firewall, as discussed above. Wong et al teaches that the routing takes place at a physical layer in the data stack, as discussed above.

As to claim 55, Wong et al teaches the method comprising:

performing a configuration integrity check of a software component on the host device [column 2 line 18 to column 3 line 44].

As to claim 56, Wong et al teaches that the configuration integrity check is performed before the network connection is allowed and wherein the connection is allowed only if the configuration integrity check passes [column 2 line 18 to column 3 line 44].

As to claim 57, Wong et al teaches the method further comprising:

performing the configuration integrity check by performing a hash on the software component to produce a hash value and comparing the hash value with a stored hash value [column 2 line 18 to column 3 line 44].

As to claim 58, Wong et al teaches that the stored hash value resides on the firewall device [column 2 line 18 to column 3 line 44].

As to claim 59, Wong et al teaches the method further comprising:

f) sending an alert if the configuration integrity check fails [column 5 line 59 to column 6 line 37].

As to claim 60, Wong et al teaches the method further comprising:

g) storing an alert if the configuration integrity check fails [column 5 line 59 to column 6 line 37].

As to claim 62, Wong et al teaches transferring data to be transferred over the network by the communication interface device to the firewall device, as discussed above. Wong et al teaches processing the data with the hardware-implemented firewall, as discussed above. Wong et al teaches that the data is processed by the hardware-implemented firewall before it is transferred over the network connection established via the communication interface device, as discussed above.

10. Claims 31 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al et al U.S. Patent No. 6,389,419 B1 as applied to claims 26 and 40 above, and further in view of Hallinan et al et al U.S. Patent No. 6,996,614 B2.

As to claims 31 and 47, Wong et al teaches g) the communication interface device transferring data received from the network in b) to the firewall device [column 6 line 47 to

column 7 line 2]. Wong et al teaches that the firewall device processes the data with the hardware implemented firewall [column 6 line 47 to column 7 line 2].

Wong et al does not teach f) swapping resource spaces in the host device that are reserved for the communication interface device and the firewall device. Wong et al does not teach that the host device treats the communication interface as the firewall device and vice versa.

Hallinan et al teaches swapping resource spaces in a host device [column 7 line 13 to column 8 line 13].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al so that there would have been a step to swap resource space in a host device that was reserved for the communication device and the firewall device. The host device would have treated the communication device as the firewall device and vice versa. The communication interface device would have transferred data received from the network to the firewall device. The hardware implemented firewall would have processed the data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Wong et al by the teaching of Hallinan et al because selection of inappropriate resources resulting in additional resources being obtained from the service provider to satisfy subsequent resource requests, and the consequent accumulation of resources in the resource pool, can be avoided [column 4, lines 45-67].

11. Claim 61 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al et al U.S. Patent No. 6,389,419 B1 and Mayer U.S. Patent No. 7,003,562 B2 as applied to claim 52 above, and further in view of Hallinan et al et al U.S. Patent No. 6,996,614 B2.

As to claims 31, 47 and 61, the Wong-Mayer combination teaches g) the communication interface device transferring data received from the network in b) to the firewall device [column 6 line 47 to column 7 line 2]. The Wong-Mayer combination teaches that the firewall device processes the data with the hardware implemented firewall [column 6 line 47 to column 7 line 2].

The Wong-Mayer combination does not teach f) swapping resource spaces in the host device that are reserved for the communication interface device and the firewall device. The Wong-Mayer combination does not teach that the host device treats the communication interface as the firewall device and vice versa.

Hallinan et al teaches swapping resource spaces in a host device [column 7 line 13 to column 8 line 13].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Wong-Mayer combination so that there would have been a step to swap resource space in a host device that was reserved for the communication device and the firewall device. The host device would have treated the communication device as the firewall device and vice versa. The communication interface device would have transferred data received from the network to the firewall device. The hardware implemented firewall would have processed the data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Wong-Mayer combination by the teaching of Hallinan

et al because selection of inappropriate resources resulting in additional resources being obtained from the service provider to satisfy subsequent resource requests, and the consequent accumulation of resources in the resource pool, can be avoided [column 4, lines 45-67].

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
March 27, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100